

FIG. 1

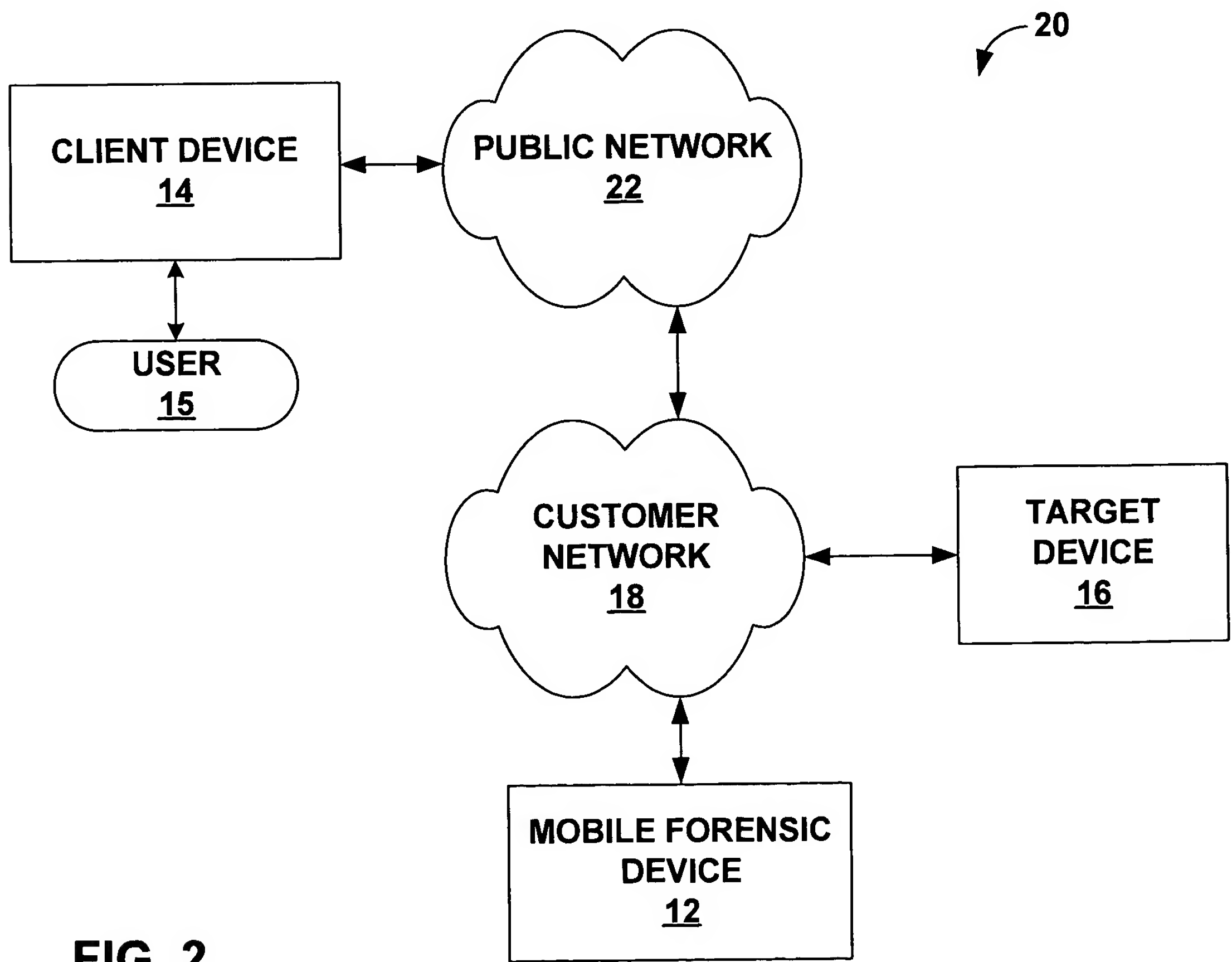


FIG. 2

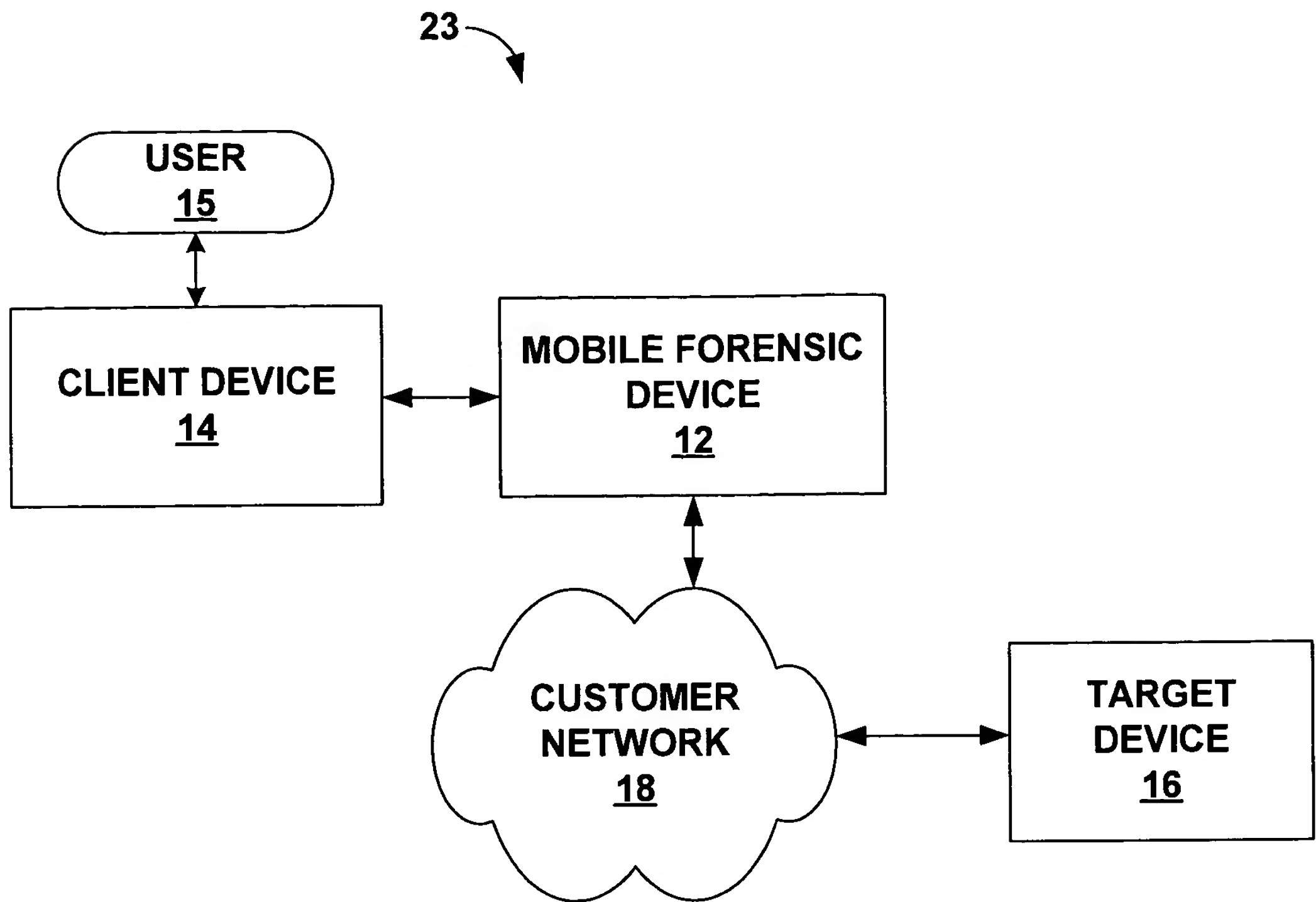
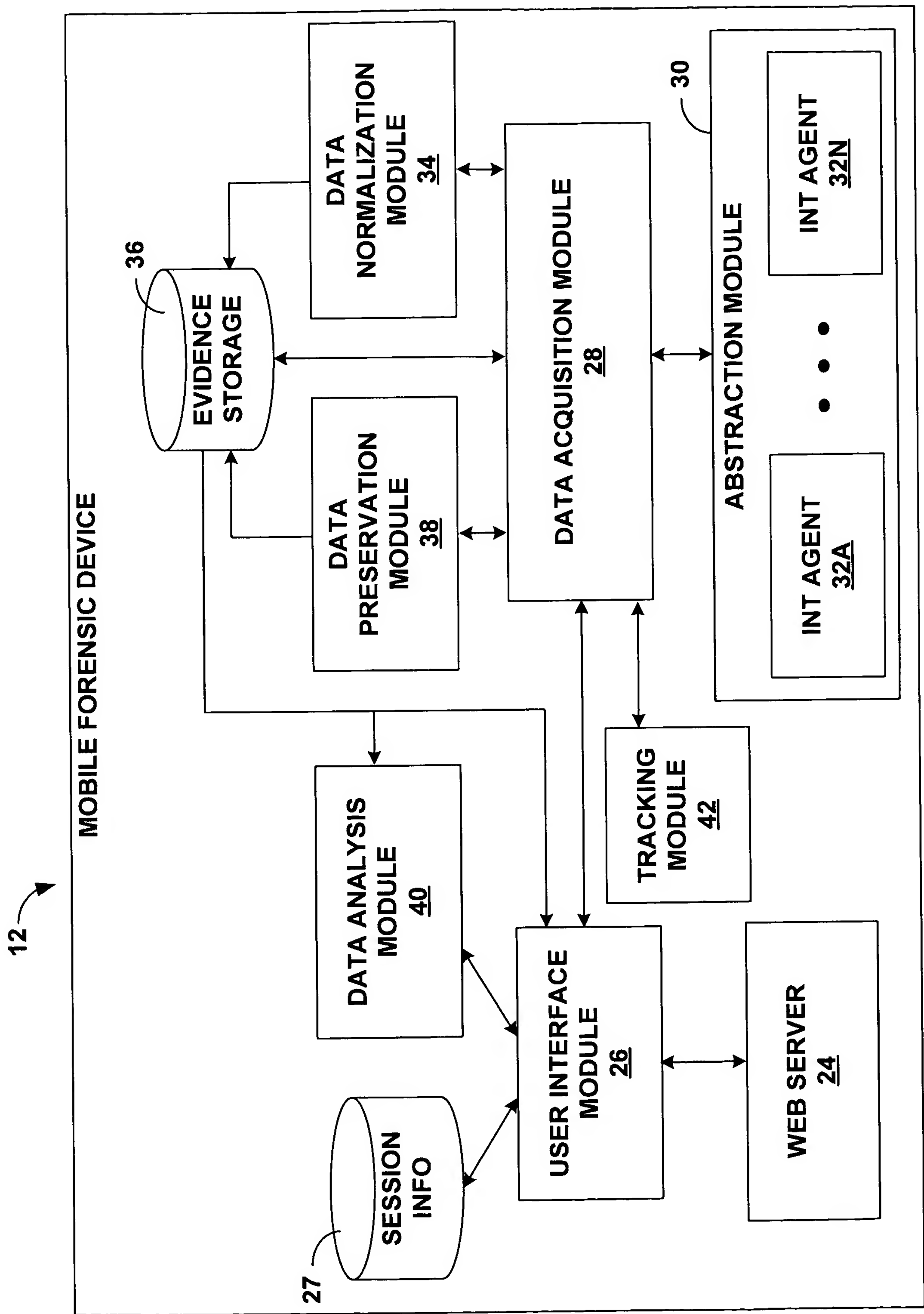
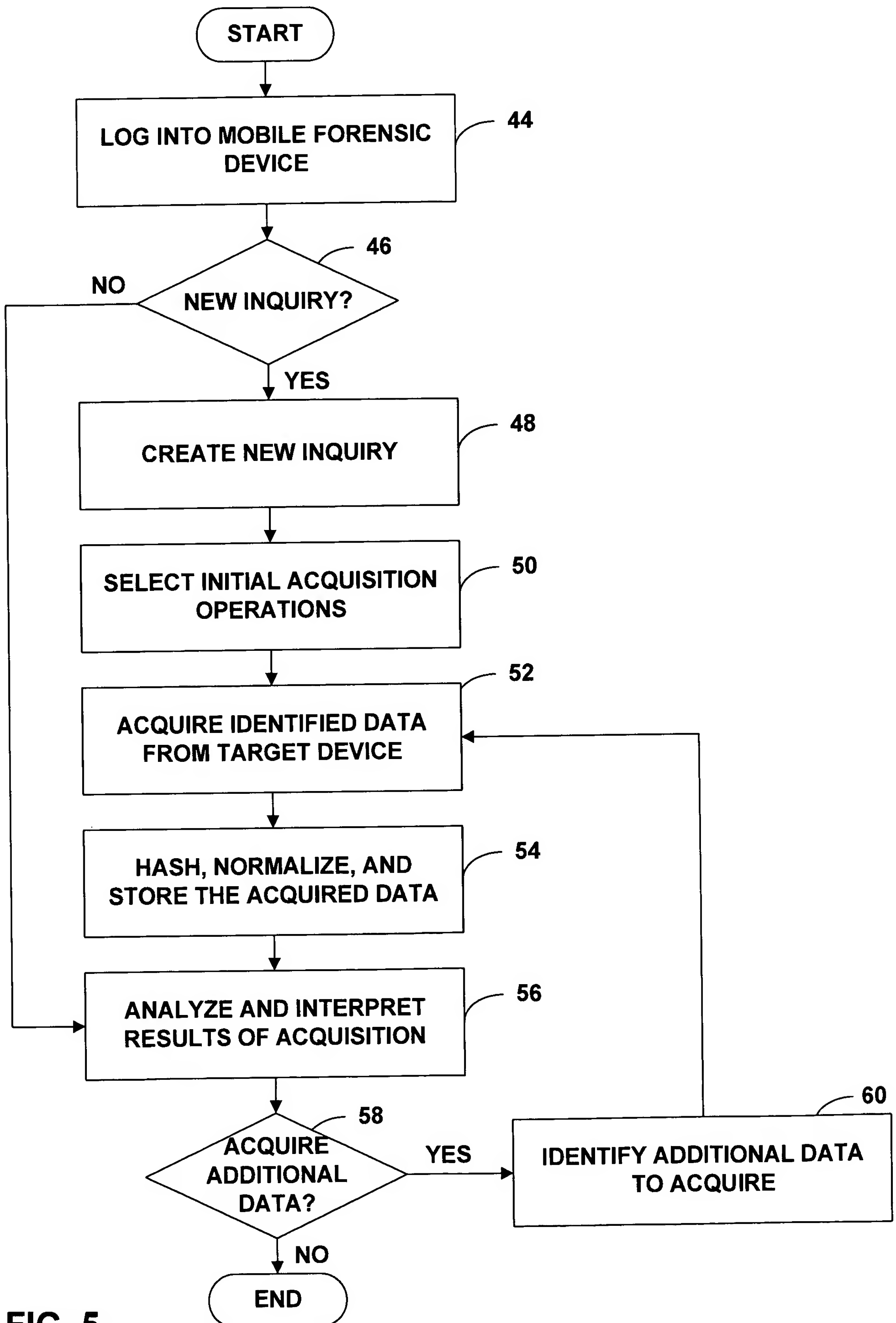
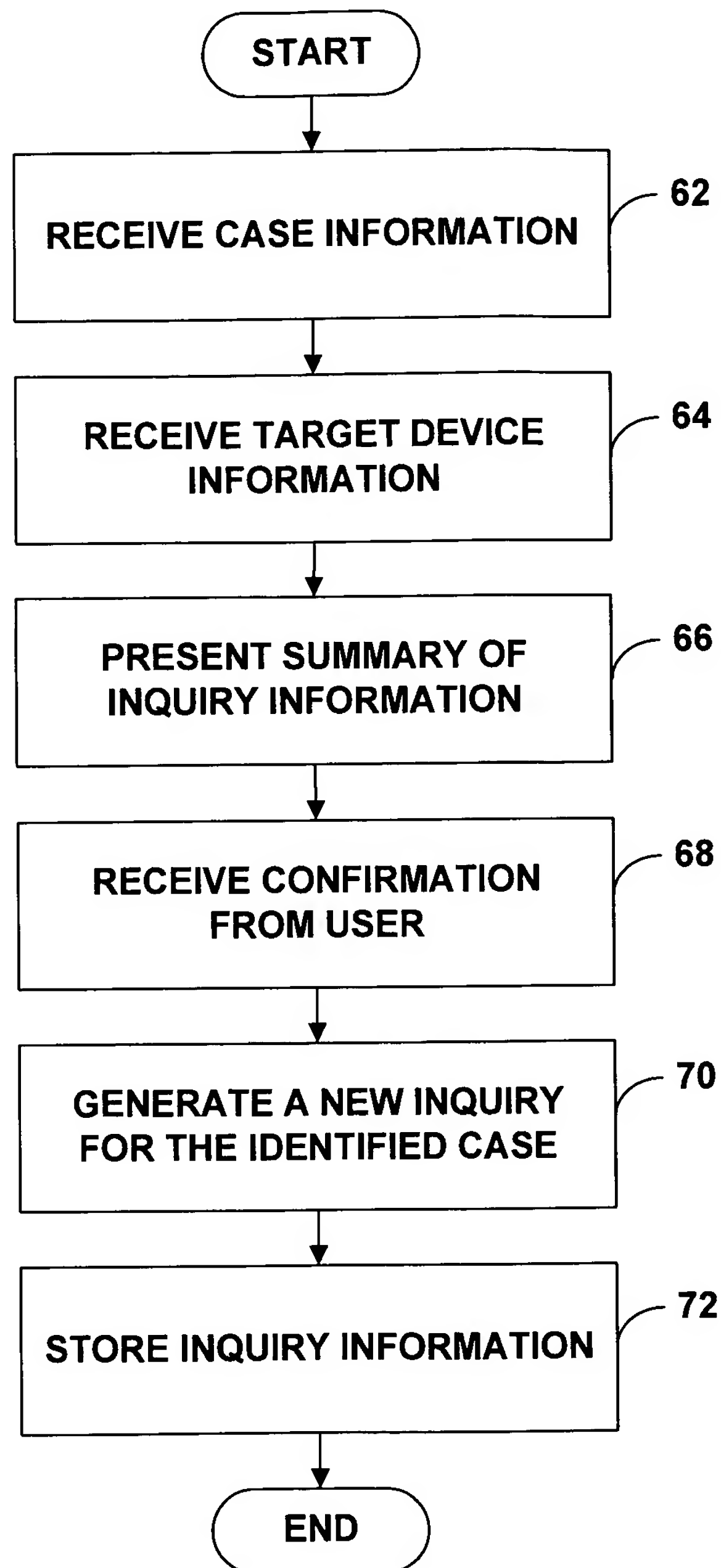


FIG. 3





**FIG. 5**



**FIG. 6**

74

MFP: Create Mobile Forensic Inquiry (MFI) - Mozilla

File Edit View Go Bookmarks Tools Window Help

### Create Mobile Forensic Inquiry (MFI)

Fill in this form and click Save to start a new MFI. Except for "Additional Information," all fields are required.

Case number:

Case title:

Principal investigator:

MFI number or mnemonic:

Location for data and evidence:

Time zone for date/time reporting:

Additional information:

80

78

82

Logged in user: rob [account mgmt](#)

[Log out](#)  
[Select/Create MFI](#)  
[View MFP log](#)

Done

FIG. 7

76

MFP: Target Machine Information - Mozilla

File Edit View Go Bookmarks Tools Window Help

### Target Machine Information

Please describe the target machine for the new inquiry (case number: 463352, MFI: demo at 3:35pm). Except for "Additional info," all fields are required.

Host name or IP address:

Operating system:

User to log in as:   
This user must have Administrative/root privilege on the target machine.

Account location: ☐ Local machine account, or  
☒ Account in the Windows domain:

Access methods to use: ☒ Windows Management Instrumentation (WMI)  
☒ SMB/CIFS  
☒ SSH/SCP  
☒ RSH/RCP  
☒ NFS  
☒ FTP  
☒ HTTP

Additional info about the machine:

84

86

80

Logged in user: rob [\[account mgmt\]](#)

[Log out](#)  
[Select/Create MFI](#)  
[View MFP log](#)

Done

FIG. 8

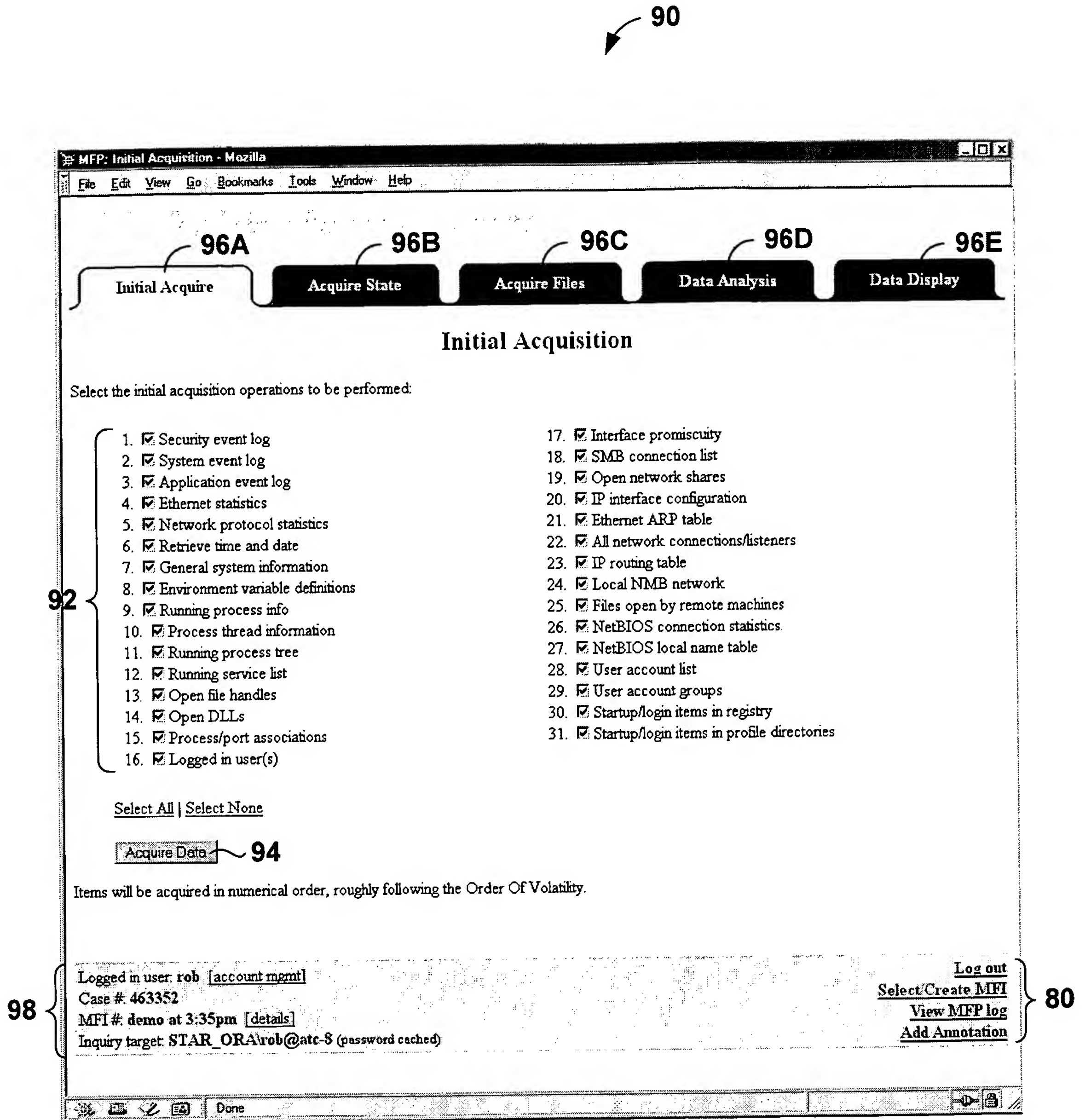
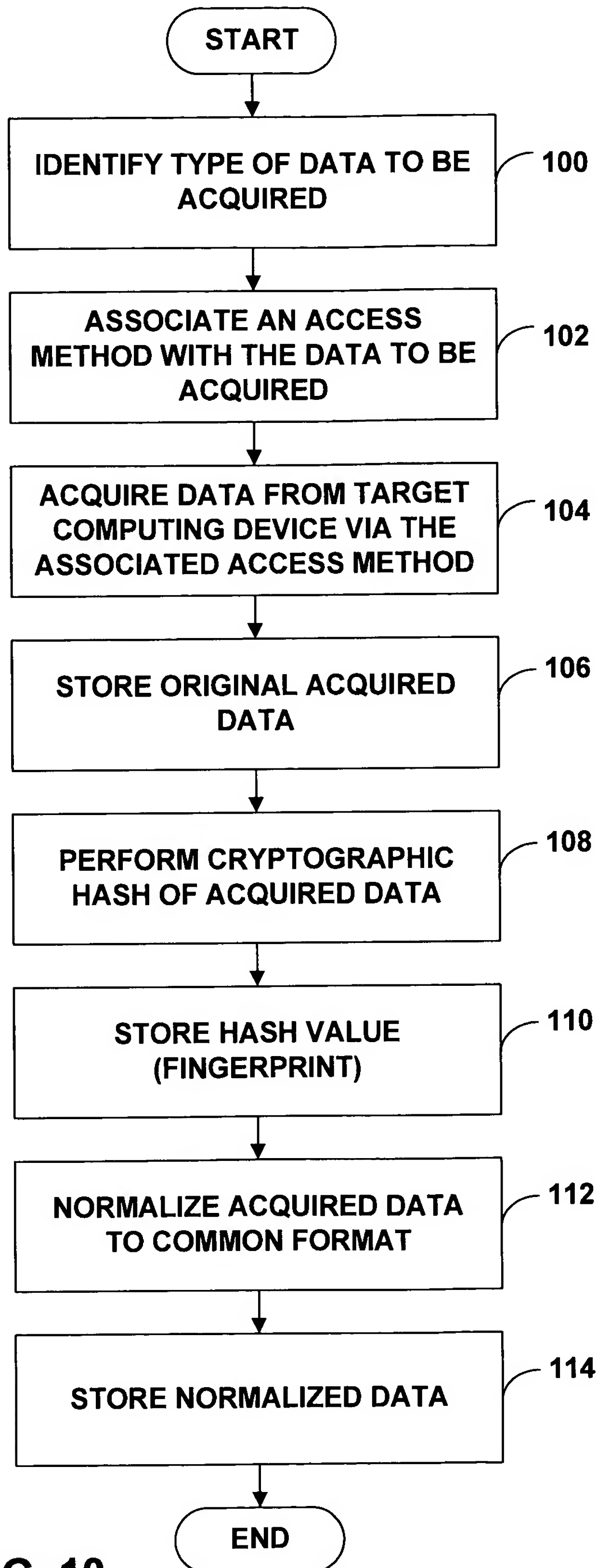
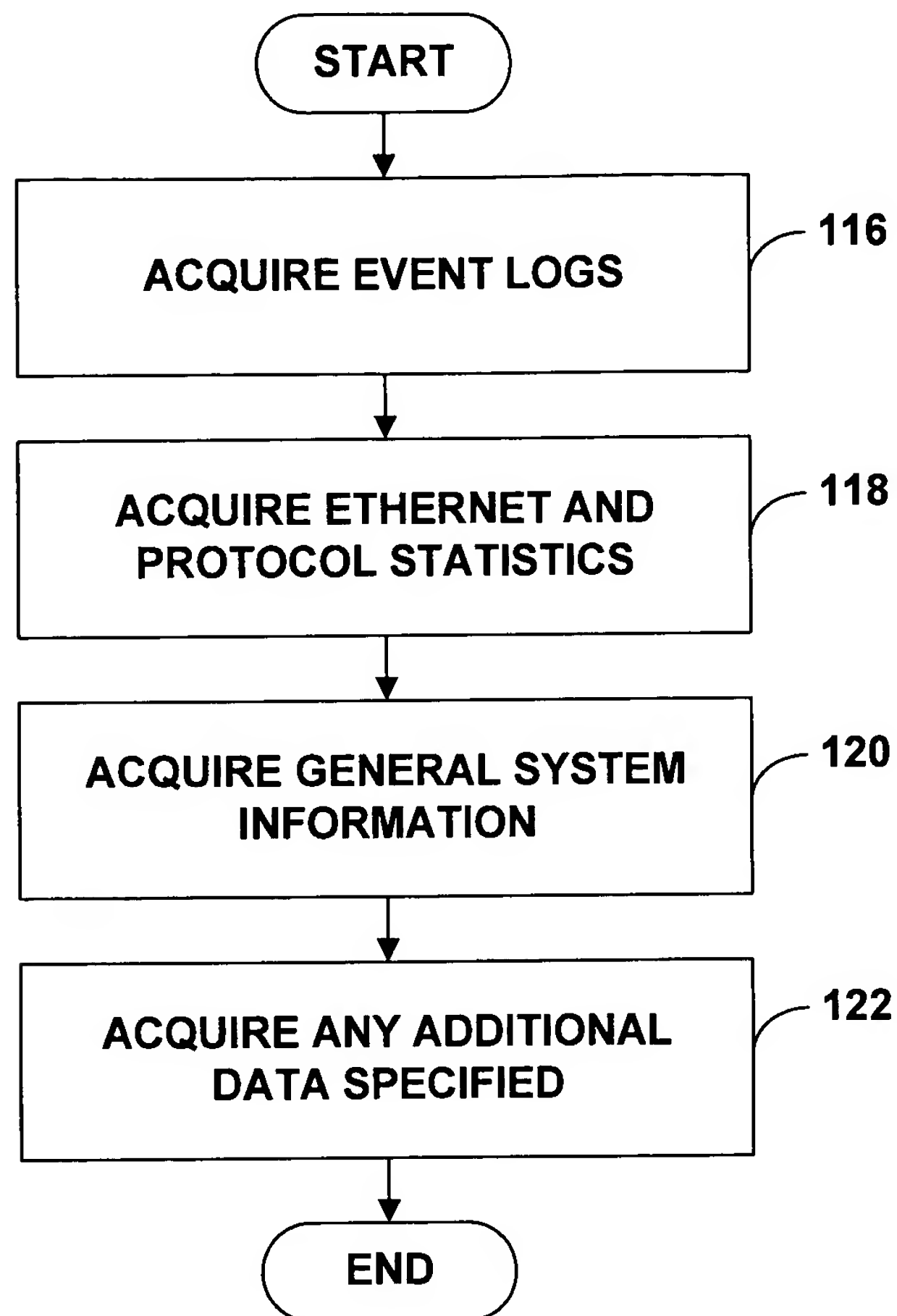


FIG. 9





**FIG. 10**



**FIG. 11**

126

MFP: Running Processes - Mozilla

File Edit View Go Bookmarks Tools Window Help

Initial Acquire Acquire State Acquire Files Data Analysis Data Display

### Running Processes

Click on a column heading to sort by that column. The current sort column is indicated in bold and by ascending/descending bars; to reverse the direction of the sort, click that column's heading.

More detailed information about a particular process is available by clicking on that process's name in the first column. Times are given in hhh:mm:ss msec format, and start times are corrected to the MFP's clock.

Processes running during initial acquire:

Number of processes: 45

Process Name	ID	Priority	# of Threads	# File Handles	Memory Use (KB)	User Time	Kernel Time	Elapsed Time	Start Time
System Idle Process	0	0	1	0	16	0:0:0.0	307:13:8.94	-	-
System	8	8	44	220	217	0:0:0.0	0:1:42.953	-	-
EXPLORER.EXE	148	8	16	633	6263	0:0:30.297	0:0:47.313	310:53:14.31	Thu May 08 16:44:26 EDT 2003
SMSS.EXE	176	11	6	33	647	0:0:0.16	0:0:0.703	310:54:13.219	Thu May 08 16:43:27 EDT 2003
WINLOGON.EXE	196	13	17	372	3396	0:0:0.672	0:0:2.422	310:53:52.156	Thu May 08 16:43:48 EDT 2003
CSRSS.EXE	200	13	10	477	1389	0:0:0.906	0:1:10.406	310:53:54.78	Thu May 08 16:43:46 EDT 2003
SERVICES.EXE	248	9	37	637	13709	0:0:3.250	0:0:9.609	310:53:51.313	Thu May 08 16:43:49 EDT 2003
LSASS.EXE	260	9	19	325	2339	0:0:0.734	0:0:1.609	310:53:51.297	Thu May 08 16:43:49 EDT 2003
rxvt.exe	336	8	4	91	1262	0:0:0.828	0:0:2.297	292:28:36.266	Fri May 09 11:09:04 EDT 2003
SVCHOST.EXE	440	8	11	372	4932	0:0:0.172	0:0:0.281	310:53:48.391	Thu May 08 16:43:52 EDT 2003
SPOOLSV.EXE	472	8	13	221	7999	0:0:1.47	0:0:1.313	310:53:48.219	Thu May 08 16:43:52 EDT 2003
SVCHOST.EXE	540	8	22	308	8086	0:0:0.172	0:0:0.766	310:53:41.672	Thu May 08 16:43:59 EDT 2003
mdm.exe	564	8	4	108	3670	0:0:0.250	0:0:0.313	310:53:41.266	Thu May 08 16:43:59 EDT 2003
AcroTray.exe	600	8	1	32	1618	0:0:0.16	0:0:0.78	310:53:10.31	Thu May 08 16:44:30 EDT 2003
mozilla.exe	616	8	15	299	37724	0:4:28.938	0:1:58.938	310:52:57.969	Thu May 08 16:44:43 EDT 2003
REGSVCS.EXE	644	8	2	31	1249	0:0:0.31	0:0:0.63	310:53:40.31	Thu May 08 16:44:00 EDT 2003
MSTASK.EXE	664	8	6	117	3703	0:0:0.31	0:0:0.63	310:53:39.719	Thu May 08 16:44:01 EDT 2003
SVCHOST.EXE	684	8	7	226	12018	0:0:1.521	0:0:1.16	310:52:30.0	Thu May 08 16:44:02 EDT 2003

FIG. 12

128

MFP: Detailed Process Information - Mozilla

File Edit View Go Bookmarks Tools Window Help

Initial Acquire Acquire State Acquire Files Data Analysis Data Display

### Detailed Process Information

In each table below, click on a heading to sort by that column, and click on it again to reverse the sort order. All start times are corrected to the MFP's clock.

**Process info:**

Process Name: winword  
Process ID: 1220  
Owner/Context: STAR\_ORA\rob  
Command Line: "c:\Documents and Settings\rob\Desktop\cap\winword.exe" -p -n ether host a:b:c:d:e:f  
Priority: 8  
Start Time: Wed May 21 15:33:44 EDT 2003

**Memory:**

Working set: 384 KB  
Working set peak: 1980 KB  
Virtual memory: 14108 KB  
Private memory: 1496 KB  
Page faults: 578  
Non-paged pool: 2  
Paged pool: 14  
Page file usage: 1496 KB

**Times**

User time: 0:00:00.031  
(hh:mm:ss.msec) Kernel time: 0:00:00.000  
Elapsed time: 0:03:57.734

(Data acquired from Wed May 21 15:37:42 EDT 2003 to Wed May 21 15:37:47 EDT 2003.)

**Open Network Ports:**

Local Address	Local Host Name	Local Port	Protocol	Remote Address	Remote Host Name	Remote Port	State
---------------	-----------------	------------	----------	----------------	------------------	-------------	-------

Done

FIG. 13A

128

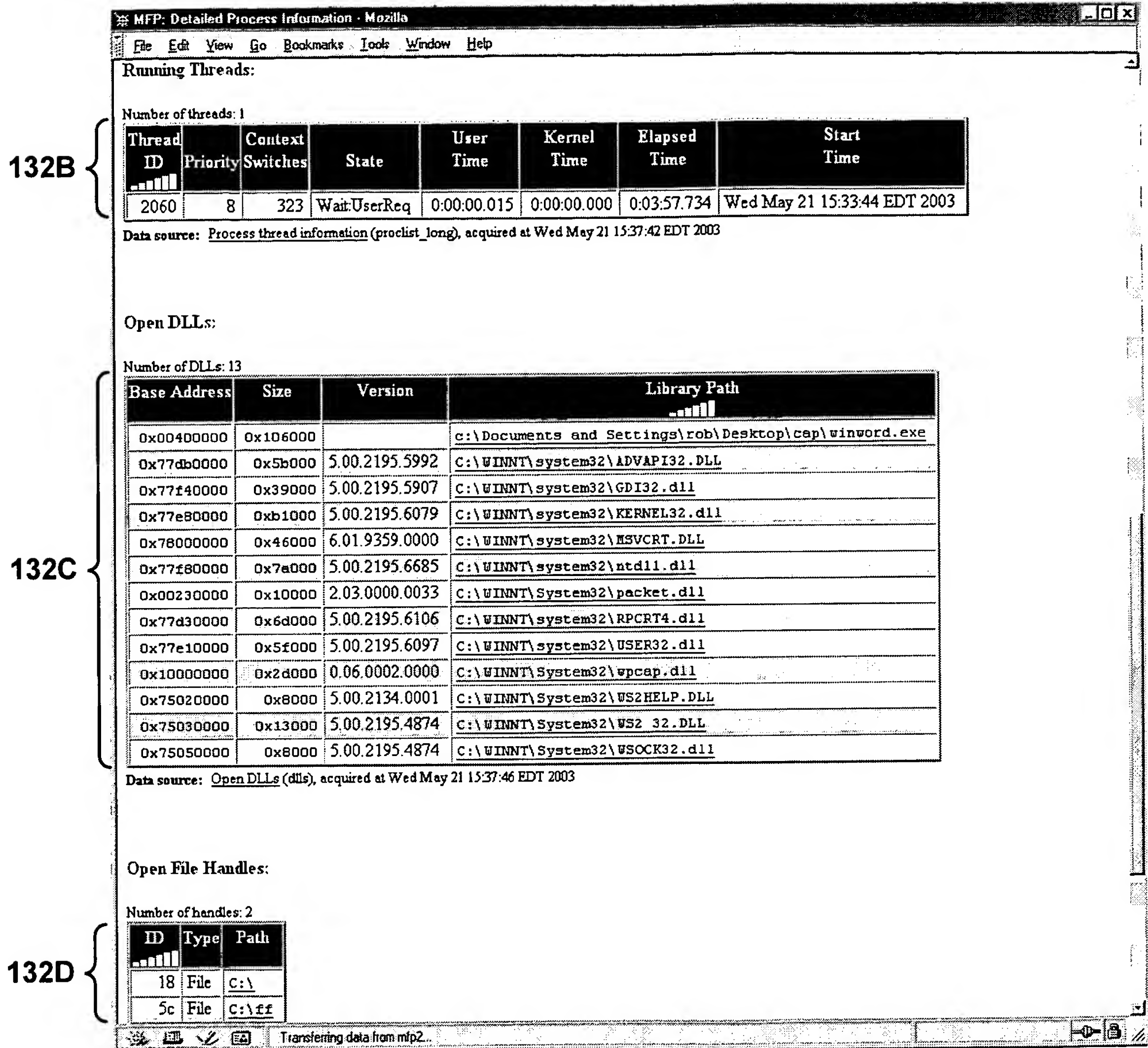
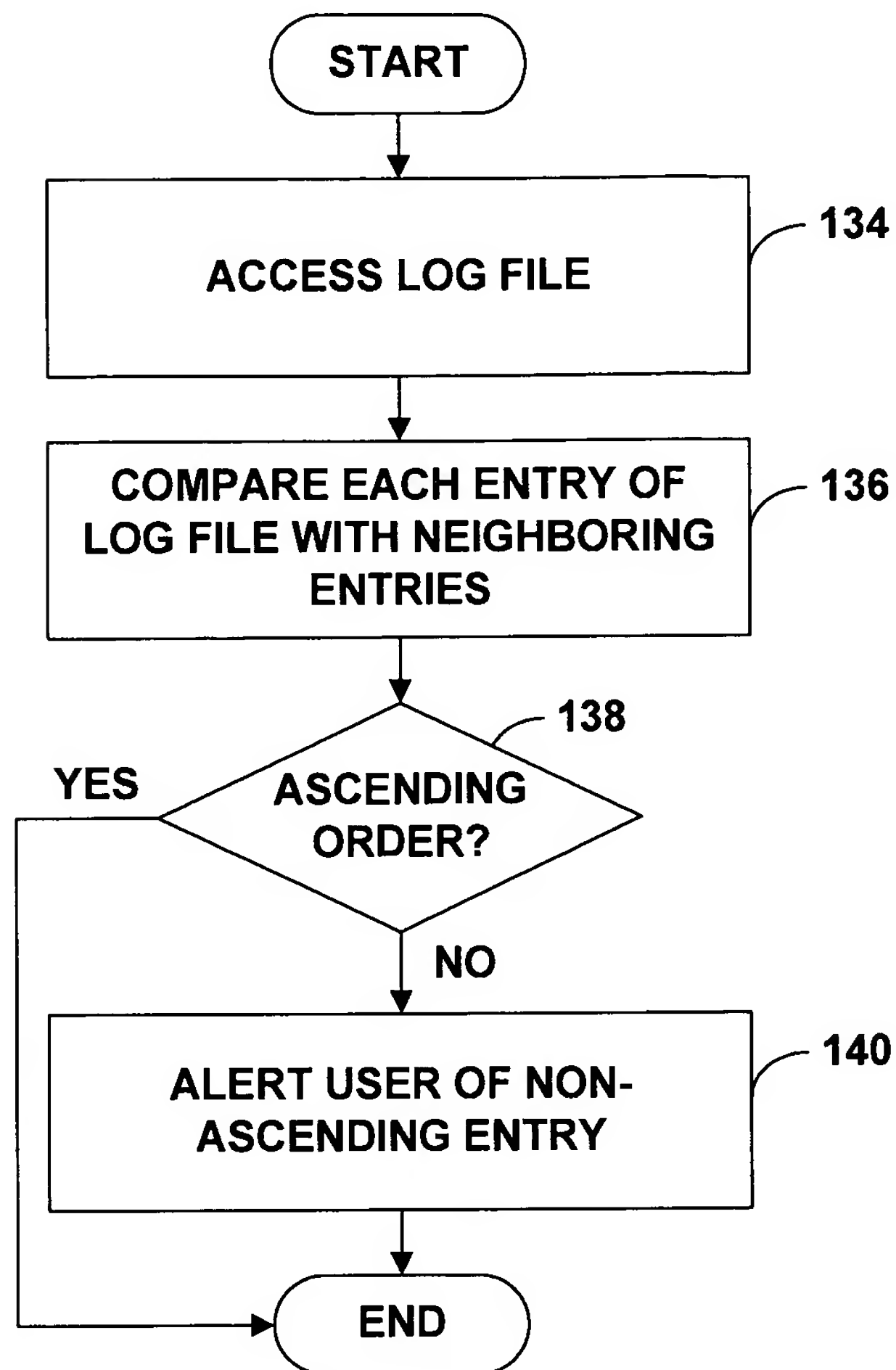
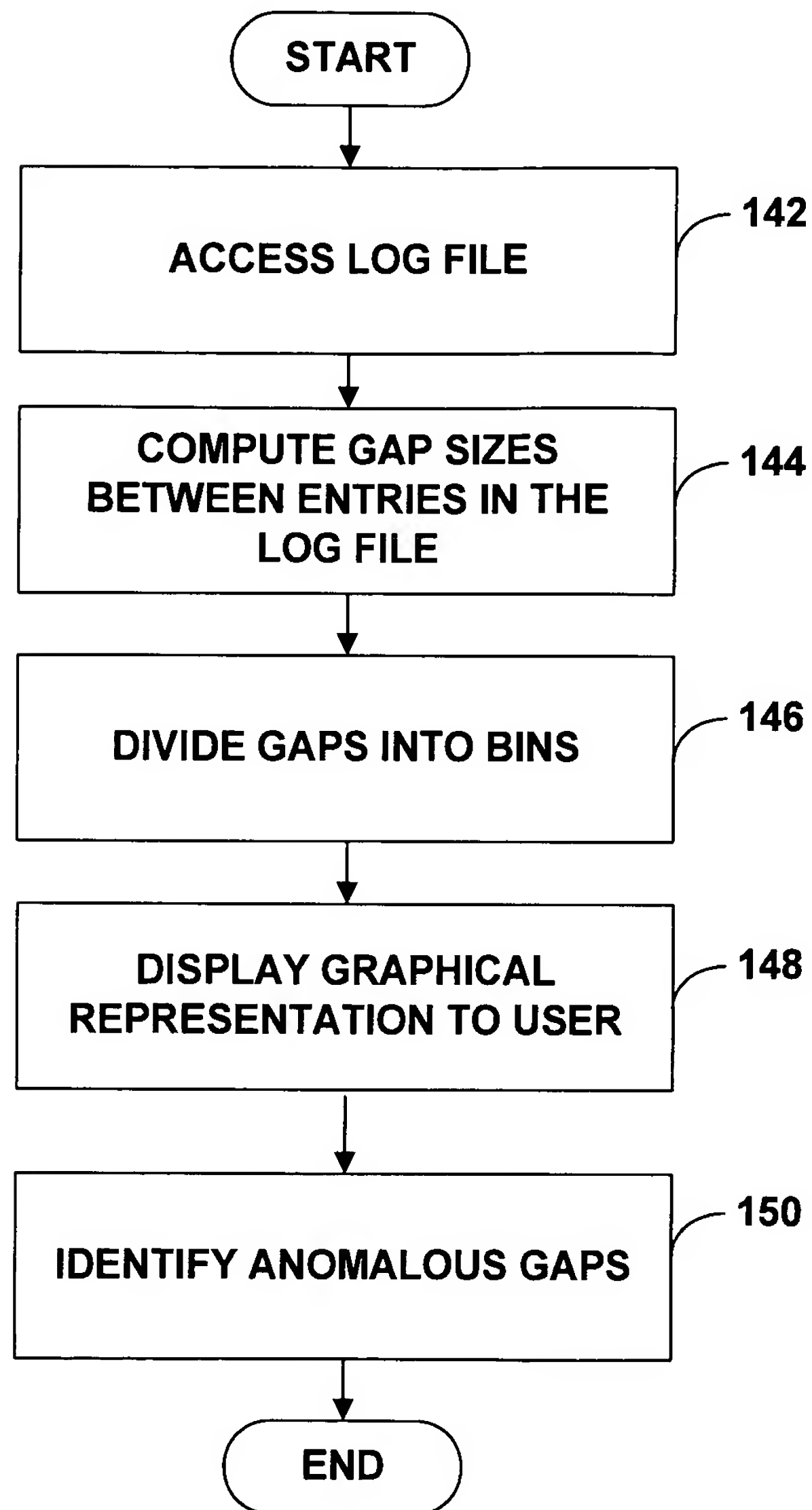


FIG. 13B



**FIG. 14**



**FIG. 15**



160

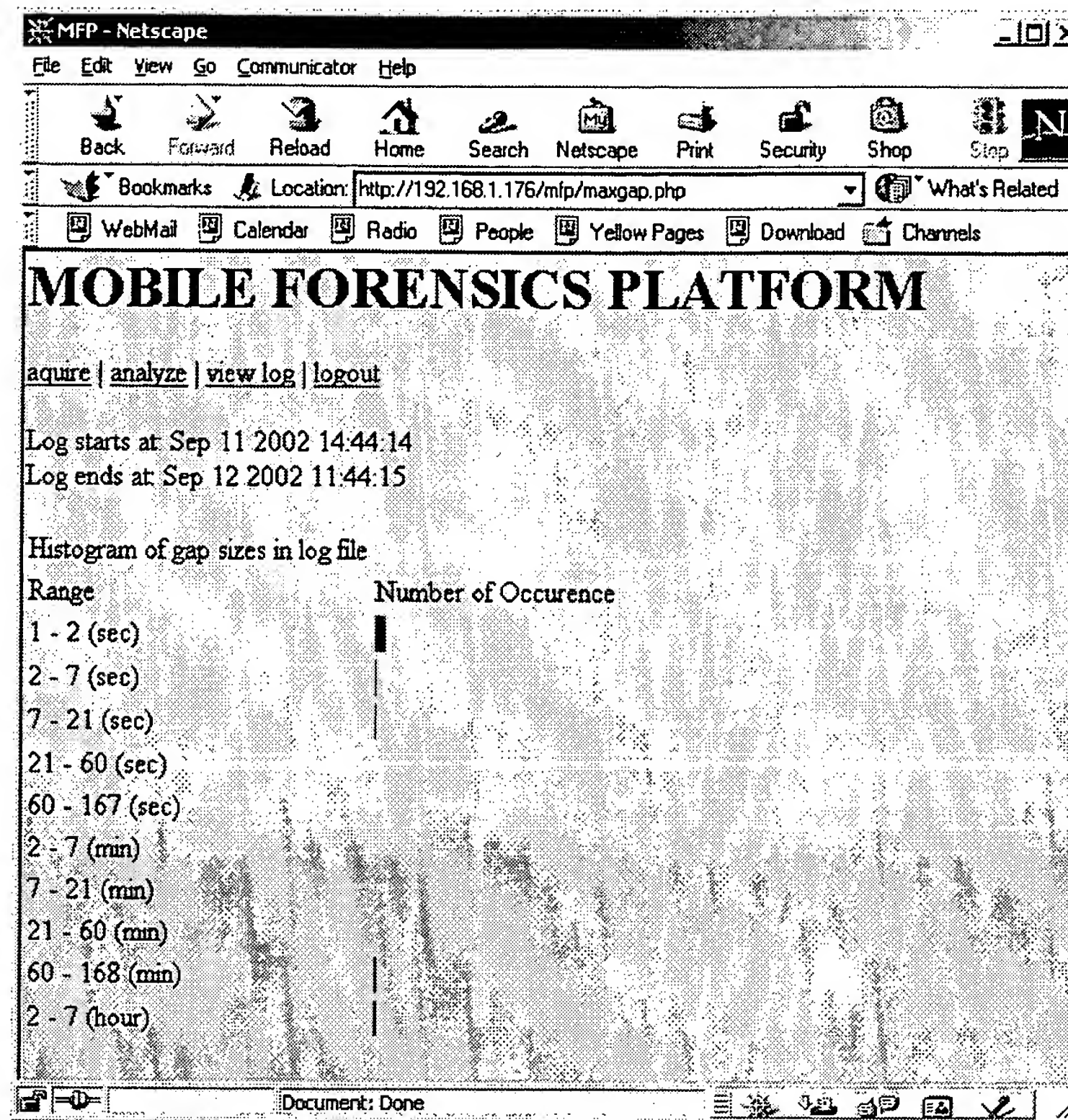
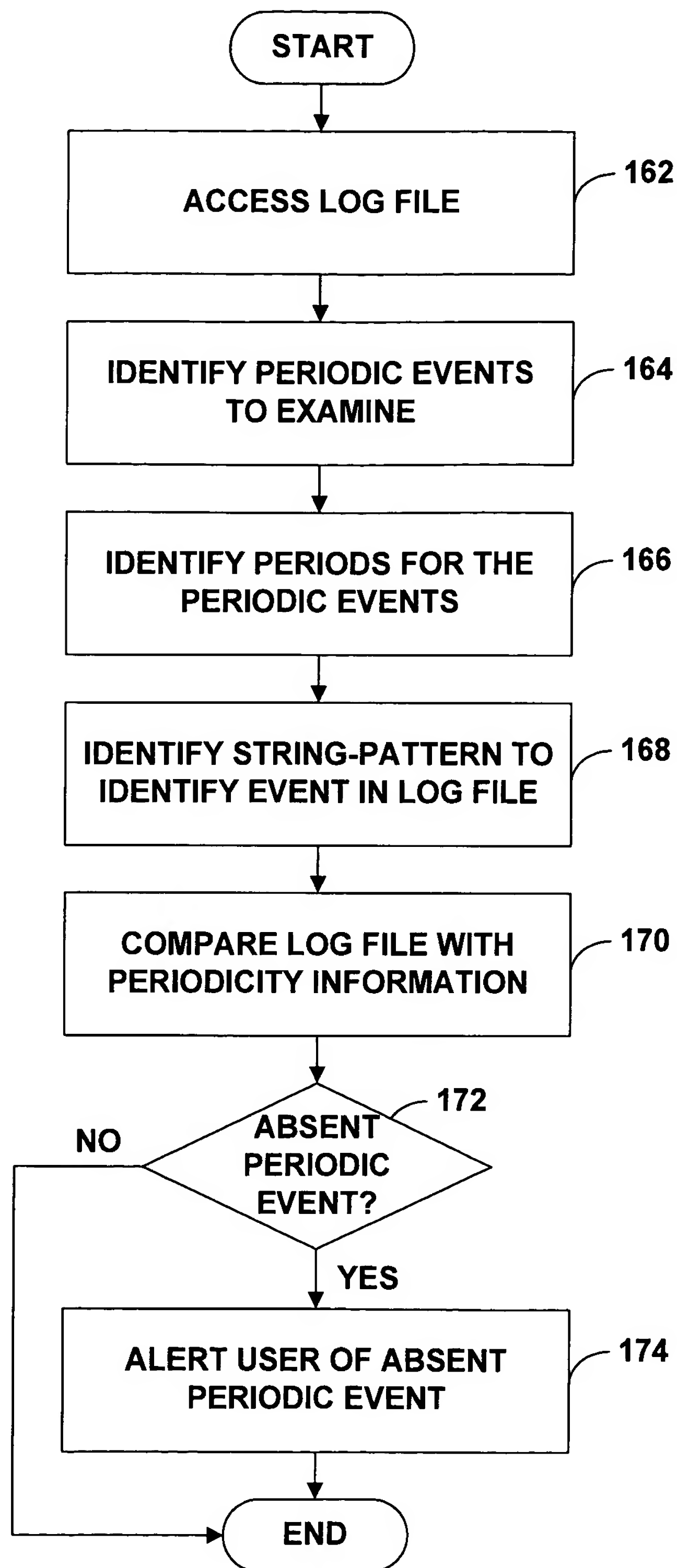


FIG. 16





**FIG. 17**